UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/316,805	05/21/1999	JOHN RAITHEL HIND	CR9-99-033	8335

25259 7590 04/30/2004

IBM CORPORATION
3039 CORNWALLIS RD.
DEPT. T81 / B503, PO BOX 12195
REASEARCH TRIANGLE PARK, NC 27709

EXAMINER	
SONG, HOSUK	

ART UNIT	PAPER NUMBER
2135	14

DATE MAILED: 04/30/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/316,805	Applicant(s) HIND ET AL.	
	Examiner Hosuk Song	Art Unit 2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 March 2004* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-6,8-14,16-22 and 24* is/are pending in the application.

4a) Of the above claim(s) *7,15 and 23* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-6,8-14,16-22,24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 3/3/2004 has been entered.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 1-6,8-14,16-22,24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Traw et al.(US 5,949,877) in view of Traw et al.(US 6,542,610) and further in view of Blumenau et al.(US 6,493,825).

Claims 1,2: Traw disclose exchanging device certificates of first and second device in (col.7,lines 7-13,37-43). Device certificate having a unique hardware id is disclosed by Traw in (col.7,lines 28-30). Traw disclose cryptographically verifying the received certificate using the public key of Certificate Authority and exchanging challenges created by each of first and second devices in (col.7,lines 25-31, 44-60). Traw disclose responding to respective challenges by signing received challenge,using the receiving device private key, private keys residing in the respective protected storage in each device and returning signed challenges in (col.7,lines 66-

67;col.lines 1-17 and col.10,lines 40-50). Traw disclose cryptographically verifying that received challenge signature is of the challenge previously sent by receiving device and establishing a key agreement between first and second devices in (col.8,lines 11-17). Traw disclose establishing secure communications if all of prior verifying steps succeed in (col.8,lines 18-29). Traw does not specifically disclose negotiating a two-way session encryption and mutual authentication requirements between first and second device. Traw patent disclose establishing initial session between first and second device and negotiating two way session encryption and mutual authentication requirements between two devices in (fig.2 and col.7,lines 6-25). It would have been obvious to person of ordinary skill in the art at the time invention was made to have pre- authenticated process as taught in Traw with device certificate method disclosed in Traw because secure communication can be achieved before actual delivery of secure contents thus adding security of its content. Further, it provides an assurance to each entity as to origin of its data sources and how data is routed to the destination thereby minimizing data compromise. Neither Traw('877) nor Traw('610) specifically discloses storing private keys in write-only storage in each device. Blumenau's patent discloses storing private keys in write only storage in each device in (col.35,lines 40-48;col.36,lines 43-46;col.37,lines 66-67). It would have been obvious to person of ordinary skill in the art at the time invention was made to employ a write-only storage to store encryption keys as taught in Blumenau with authentication system disclosed in Traw and Traw so that keys can not be read from any other external leads connected to he chip thus providing full protection of its keys against outside attacks. Further,if tampering is detected, keys can be deleted or erased thus minimizing key hacking by the intruders.

Claim 3: Traw disclose first established session is an authenticated connection in (col.8,lines 21-26).

Claim 4: Traw disclose first established session is an encrypted connection in (col.3,lines 49-52).

Claim 5: Traw disclose unique hardware identifier is a machine address in (col.10,lines 40-50).

Claim 6: Neither Traw('877) nor Traw('610) specifically discloses storing private keys in write-only storage in each device. Blumenau's patent discloses storing private keys in write only storage in each device in (col.35,lines 40-48;col.36,lines 43-46;col.37,lines 66-67). It would have been obvious to person of ordinary skill in the art at the time invention was made to employ a write-only storage to store encryption keys as taught in Blumenau with authentication system disclosed in Traw and Traw so that keys can not be read from any other external leads connected to he chip thus providing full protection of its keys against outside attacks. Further,if tampering is detected, keys can be deleted or erased thus minimizing key hacking by the intruders.

Claim 8: Traw disclose public key of a CA is a public key of a root CA in (col.10,lines 40-46).

Claims 9-14,16 differs from claims 1-8 in that computer program code is claimed. It is inherent in system of Traw,Blumenau to include a software code in order to perform cryptographic processing. The examiner asserts that performing a cryptographic functions by a computer without implementation of software is not possible.

Claims 17,18: Traw disclose exchanging device certificates of first and second device in (col.7,lines 7-13,37-43). Device certificate having a unique hardware id is disclosed by Traw in (col.7,lines 28-30). Traw disclose cryptographically verifying the received certificate using the public key of Certificate Authority and exchanging challenges created by each of first and second devices in (col.7,lines 25-31, 44-60). Traw disclose responding to respective challenges by signing received challenge,using the receiving device private key, private keys residing in the respective protected storage in each device and returning signed challenges in (col.7,lines 66-67;col.lines 1-17 and col.10,lines 40-50). Traw disclose cryptographically verifying that received challenge signature is of the challenge previously sent by receiving device and establishing a

key agreement between first and second devices in (col.8,lines 11-17). Traw disclose establishing secure communications if all of prior verifying steps succeed in (col.8,lines 18-29). Traw does not specifically disclose negotiating a two-way session encryption and mutual authentication requirements between first and second device. Traw patent disclose establishing initial session between first and second device and negotiating two way session encryption and mutual authentication requirements between two devices in (fig.2 and col.7,lines 6-25). It would have been obvious to person of ordinary skill in the art at the time invention was made to have pre- authenticated process as taught in Traw with device certificate method disclosed in Traw because secure communication can be achieved before actual delivery of secure contents thus adding security of its content. Further, it provides assurance to each entity as to origin of its data sources and how data is routed to the destination thereby minimizing data compromise. Neither Traw('877) nor Traw('610) specifically discloses storing private keys in write-only storage in each device. Blumenau's patent discloses storing private keys in write only storage in each device in (col.35,lines 40-48;col.36,lines 43-46;col.37,lines 66-67). It would have been obvious to person of ordinary skill in the art at the time invention was made to employ a write-only storage to store encryption keys as taught in Blumenau with authentication system disclosed in Traw and Traw so that keys can not be read from any other external leads connected to he chip thus providing full protection of its keys against outside attacks. Further,if tampering is detected, keys can be deleted or erased thus minimizing key hacking by the intruders.

Claim 19: Traw disclose first established session is an authenticated connection in (col.8,lines 21-26).

Claim 20: Traw disclose first established session is an encrypted connection in (col.3,lines 49-52).

Claim 21: Traw disclose unique hardware identifier is a machine address in (col.10,lines 40-50).

Claim 22: Neither Traw('877) nor Traw('610) specifically discloses storing private keys in write-only storage in each device. Blumenau's patent discloses storing private keys in write only storage in each device in (col.35,lines 40-48;col.36,lines 43-46;col.37,lines 66-67). It would have been obvious to person of ordinary skill in the art at the time invention was made to employ a write-only storage to store encryption keys as taught in Blumenau with authentication system disclosed in Traw and Traw so that keys can not be read from any other external leads connected to he chip thus providing full protection of its keys against outside attacks. Further,if tampering is detected, keys can be deleted or erased thus minimizing key hacking by the intruders.

Claim 24: Traw disclose public key of a CA is a public key of a root CA in (col.10,lines 40-46).

Conclusion

3. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Hosuk Song whose telephone number is 703-305-0042. The examiner can normally be reached on Tue-Frifrom 6:00 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

HS